Data Book

AU9530
USB eToken Controller
Technical Reference Manual

Product Specification

Preliminary Release

Revision 1.03

Confidential

May 2004

Data Sheet Status

Objective specification	This data sheet contains target or goal specifications for product development.
Preliminary specification	This data sheet contains preliminary data; supplementary data may be published later.
Product specification	This data sheet contains final product specifications.

Revision History

Date	Revision	Description
Mar 2004	1.00/A21	Initial release
Apr 2004	1.01/A21	Modify 1.2 “feature”
May 2004	1.02/A21	Modify Pin out and schematics.
May 2004	1.03/A21	Modify table “5.1 command and description”

Contact Information:

Web site: http://www.alcormicro.com/

Product URL: http://www.alcormicro.com/product_AU9530.htm

Taiwan
Alcor Micro Corp.
4F, No 200 Kang Chien Rd., Nei Hu,
Taipei, Taiwan, R.O.C.
Phone: 886-2-8751-1984
Fax: 886-2-2659-7723

Santa Clara Office
2901 Tasman Drive, Suite 206
Santa Clara, CA 95054
USA
Phone: (408) 845-9300
Fax: (408) 845-9086

Los Angeles Office
9400 Seventh St., Bldg. A2
Rancho Cucamonga, CA 91730
USA
Phone: (909) 483-9900
Fax: (909) 944-0464

Table of Contents

List of Figures

List of Tables

1.0. Introduction

1.1. Description

AU9530 is a cost-effective and easy-to-use USB single chip controller for e-commerce and network security applications. It can be extensively used in the network security solutions such as identification, network access control, digital signature for secure email and file encryption/decipher, e-Wallet in personal expenditure of internet, system login key…etc.

AU9530 is based on USB interface to take advantage of plug and play nature and rich set of driver stack support. In the meanwhile, it works with various sizes EEPROM for reading/writing access with encryption/decryption capacity to ensure security key to be protected, even when storing or transferring. The chip also supports a H/W random number generator.

In order to speed up the manufacturer's product development, AlcorMicro provides a software development kit (SDK) for AU9530. Manufacturers can easily integrate this solution for their security needs.

Network security and system access control are becoming more and more important in the world. With AU9530, manufacturers not only can make a high security solution, but also can get the cost efficiency.

1.2. Feature

- Support USB1.1 specification
- Support USB HID 1.1 specification
- Security keys in both software and firmware
- Built in multiple bits random number generator in hardware
- CPU based design for easy customization
- GPIO pin for LED
- AlcorMicro software development kit (SDK) support
- Runs at 6MHz clock
- Supported EEPROM size from 512 bytes to 64 Kbytes
  AT 24C04, 24C08, 24C16, 24C32, 24C64, 24C128, 24C256 and 24C512 compatible

1.3. Security Feature

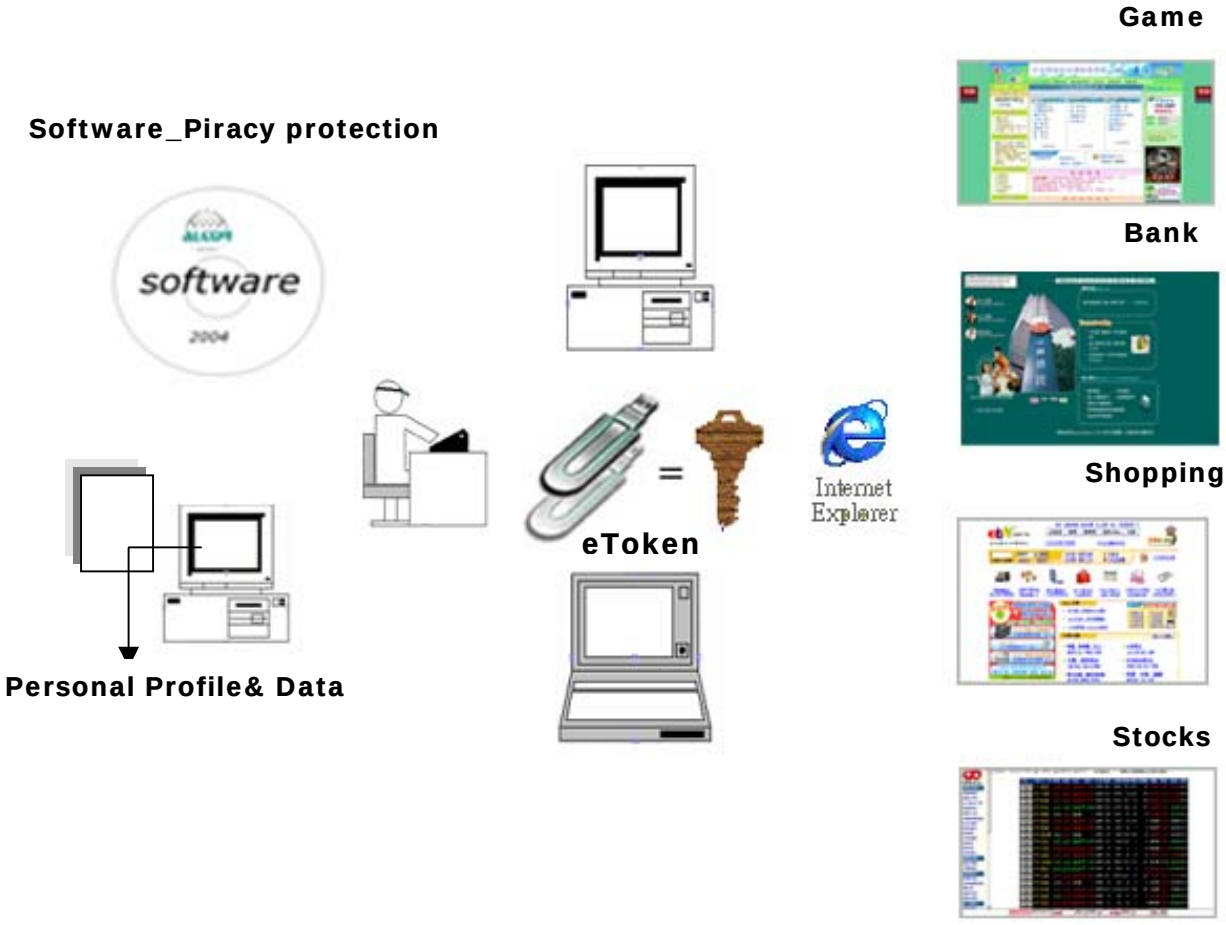
- Dynamic switch key set in per firmware command
- Hardware 3DES encryption engine for faster operation
- Authentication code password to identify users
- All data protected by hashed MAC code and checksum
- No sequence can be repeated by duplicating USB bus activity with random number function

2.0. Application Block Diagram

Following is the application diagram of a USB eToken with AU9530. By connecting the USB eToken to a desktop or notebook PC through USB bus, AU9530 is implemented as a bus-powered, full speed USB network secure device, which can be used as an authentication key, anti-piracy token or coupon storage for network security or e-commerce solution.

2.1 Block Diagram

Figure 2.1 Block Diagram



3.0. Pin Assignment

The AU9530 is packed in 20-SSOP-form factor. The following figure shows signal name for each pin and the table in the following page describes each pin in detail

Figure 3.1 Pin Assignment Diagram

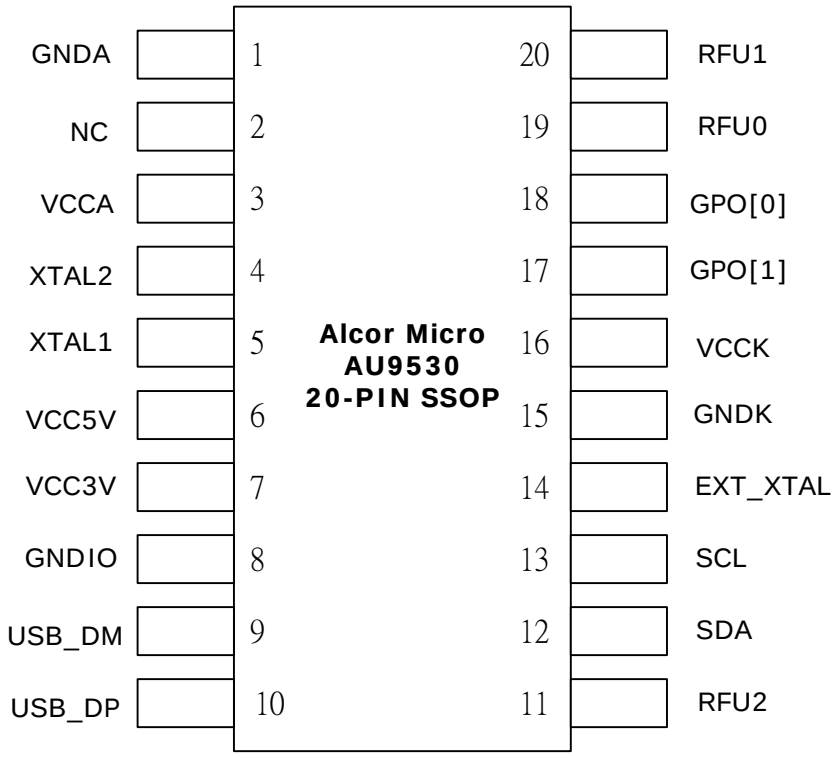


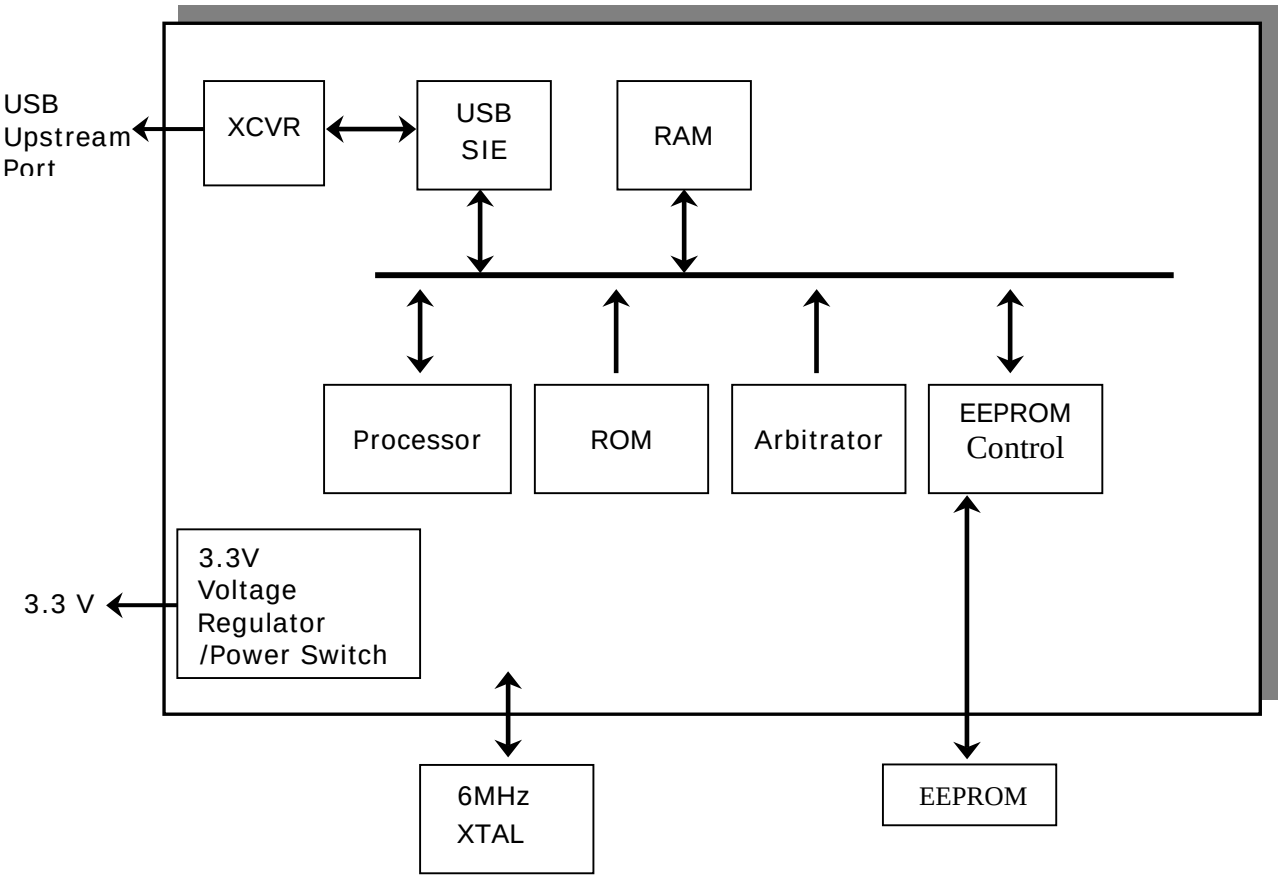
Table 3.1 Pin Descriptions

Pin	Pin Name	Type	Description
1	GNDA	PWR	Analog ground
2	NC		
3	VCCA	PWR	Analog power
4	XTAL2	O	External clock output
5	XTAL1	I	External clock input
6	VCC5V	PWR	Power supply 5V input
7	VCC3V	PWR	Power supply 3V output
8	GNDIO	PWR	Ground
9	USB_DM	I/O	USB D-, add 1.5K external pull high
10	USB_DP	I/O	USB D+
11	RFU2	I	Reserved(Always pull low)
12	SDA	I/O	EEPROM Data
13	SCL	O	EEPROM clock
14	EXT_XTAL	I	External clock Enable("1": external clock enable)
15	GNDK	PWR	Core Ground
16	VCCK	PWR	Core Power supply 3.3V
17	GPO[1]	O	General purpose Output
18	GPO[0]	O	General purpose Output
19	RFU0	I	Reserved(Always pull low)
20	RFU1	I	Reserved(Always pull low)

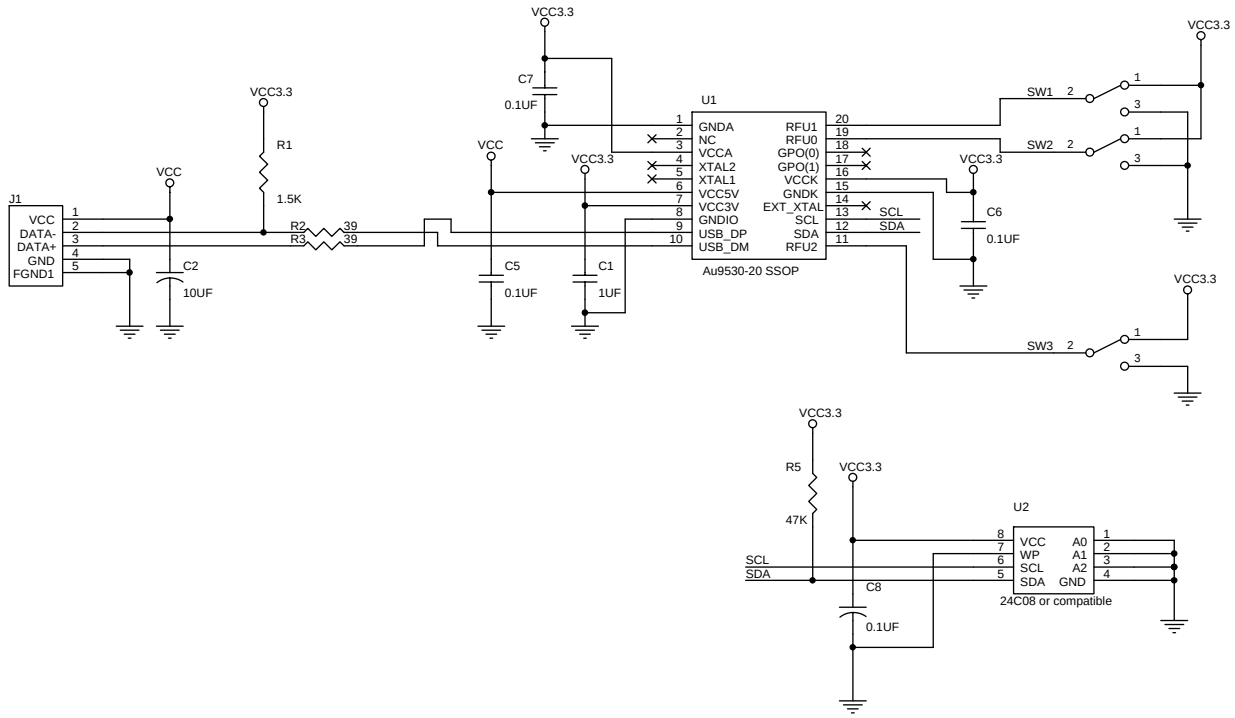
4.0. System Architecture and Reference Design

4.1. Block Diagram

Figure 4.1 AU9530 USB eToken controller Block Diagram



4.2. Sample Schematics



Disclaimer: This schematic is for reference only.
Alcor Micro Corp. makes no warranty for the use of its products and bears no responsibility for any error that appear in this document. Specifications are subject to change without notice.

Size	Document Number	Rev
A	Au9530 demostration schematic	*1.02*
Date: Thursday, May 20, 2004	Sheet 1 of 1	

5.0. API Command Set

5.1. Command Format

USB eToken with AU9530 is defined as a standard USB HID CLASS device. All commands will be wrapped in SET_REPORT data. I.e. COMMANDS are received by firmware via control pipe using SET_REPORT. Input Data received via GET_REPORT command.

5.2. Command and Description

Table 5.1 API Command Set and Description

◆ **General operation commands**	
Lock device	Disable access to all USB eToken EEPROM access commands except Unlock and Lock Status commands.
Unlock device	Enable access to USB eKey
Get Device Lock status	Return status of lock status
Get Serial Number	16 byte serial number reside in EEPROM
Write Serial Number	This is a write once command. Once written, serial number can only be erased with Erase Entire EEPROM command
Erase entire EEPROM	Erase entire EEPROM
Get Random Number	Hardware provides 4 bits random number. Firmware must read Random number 16 times to assembly a 8-bytes random number.
◆ **Block mode operation commands**	
Read block	Read multiple byte block at once with specified starting address and byte length
Write block	Write multiple byte block at once with specified starting address and byte length
◆ **Block secured mode operation commands**	
Get Session key	Exchange a 16 bytes key used for COMMAND MAC code authentication
Read 3DES block	Write 32 bytes of information with 3DES encryption with 16 bytes key
Write 3DES block	Read 32 bytes of information with 3DES encryption with 16 bytes key

6.0. Electronic Characteristics

6.1 Recommended Operation Condition

Table 6.1 Recommended Operation Condition

SYMBOL	PARAMETER	MIN	TYP	MAX	UNITS
V_{CC}	Power Supply	4.75	5	5.25	V
V_{IN}	Input Voltage	0		V_{CC}	V
T_{OPR}	Operating Temperature	0		85	^{O}C
T_{STG}	Storage Temperature	-40		125	^{O}C

6.2 General DC Characteristics

Table 6.2 General DC Characteristics

SYMBOL	PARAMETER	CONDITIONS	MIN	TYP	MAX	UNITS
I_{IL}	Input low current	no pull-up or pull-down	-1		1	μA
I_{IH}	Input high current	no pull-up or pull-down	-1		1	μA
I_{OZ}	Tri-state leakage current		-10		10	μA
C_{IN}	Input capacitance			5		ρF
C_{OUT}	Output capacitance			5		ρF
C_{BID}	Bi-directional buffer capacitance			5		ρF

6.3 DC Electrical Characteristics for 3.3 volts operation

Table 6.3 DC Electrical Characteristics for 3.3 volts operation

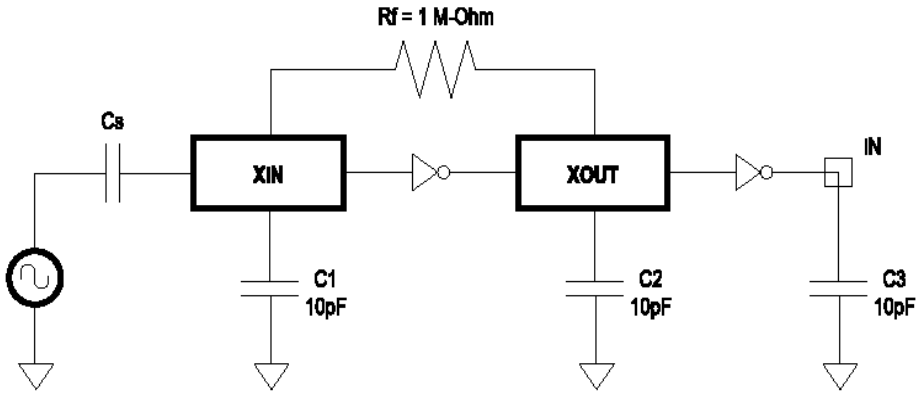
SYMBO	PARAMETER	CONDITIONS	MIN	TYP	MAX	UNITS
V_{IL}	Input Low Voltage	CMOS			0.9	V
V_{IH}	Input Hight Voltage	CMOS	2.3			V
V_{OL}	Output low voltage	I_{OL}=4mA, 16mA			0.4	V
V_{OH}	Output high voltage	I_{OH}=4mA,16mA	2.4			V

R_I	Input Pull-up/down resistance	Vil=0_V or Vih=V_{CC}		10K/200K		KΩ

6.4 Crystal Oscillator Circuit Setup for Characterization

The following setup was used to measure the open loop voltage gain for crystal oscillator circuits. The feedback resistor serves to bias the circuit at its quiescent operating point and the AC coupling capacitor, Cs, is much larger than C1 and C2.

Figure 6.1 Crystal Oscillator Circuit Setup for Characterization



6.5 ESD Test Results

Test Description: ESD Testing was performed on a Zapmaster system using the Human-Body-Model (HBM) and Machine-Model (MM), according to MIL-STD 883 and EIAJ IC-121 respectively.

- Human-Body-Model stresses devices by sudden application of a high voltage supplied by a 100pF capacitor through 1.5k-ohm resistance.
- Machine-Model stresses devices by sudden application of a high voltage supplied by a 200pF capacitor through very low (0 ohm) resistance.

Test Circuit & Condition

- Zap Interval: 1 second
- Number of Zaps: 3 positive and 3 negative at room temperature
- Criteria: I-V Curve Tracing

Table 6.4 ESD Data

Model	Mode	S/S	Target	Results
HBM	Vdd, Vss, I/C	15	6000V	PASS
MM	Vdd, Vss, I/C	15	200V	PASS

6.6 Latch-Up Test Results

Test Description: Latch-Up testing was performed at room ambient using an IMCS-4600 system which applies a stepped voltage to one pin per device with all other pins open except Vdd and Vss which were biased to 5Volts and ground respectively.

Testing was started at 5.0V (Positive) or 0V (Negative), and the DUT was biased for 0.5 seconds.

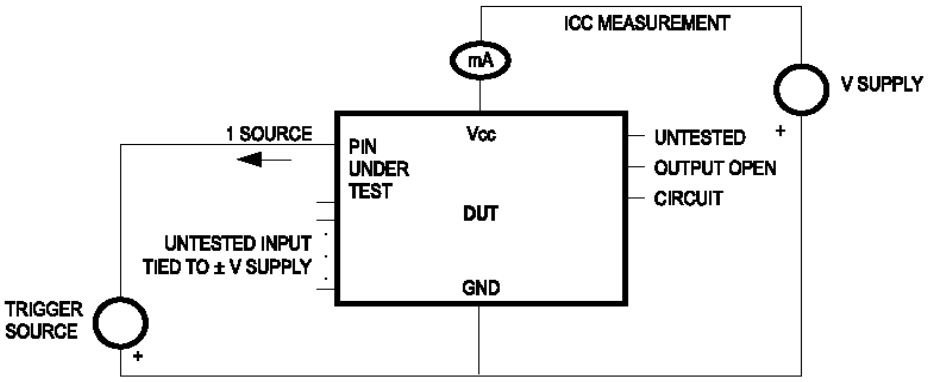
If neither the PUT current supply nor the device current supply reached the predefined limit (DUT=00mA, Icc=100mA), then the voltage was increased by 0.1Volts and the pin was tested again.

This procedure was recommended by the JEDEC JC-40.2 CMOS Logic standardization committee.

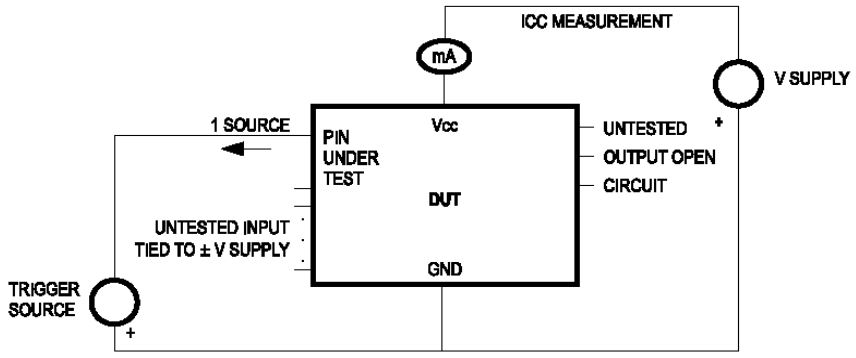
Notes:

1. DUT: The device under test.
2. PUT: The pin under test.

Figure 6.2 Latch-Up Test Results Diagram

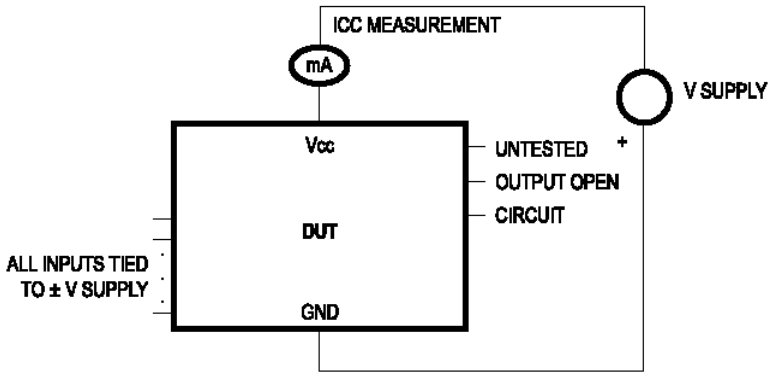


Test Circuit: Positive Input/Output Overvoltage/Overcurrent



Test Circuit: Negative Input/Output Overvoltage/Overcurrent

Figure 6.2 Latch-Up Test Results Diagram (continue)



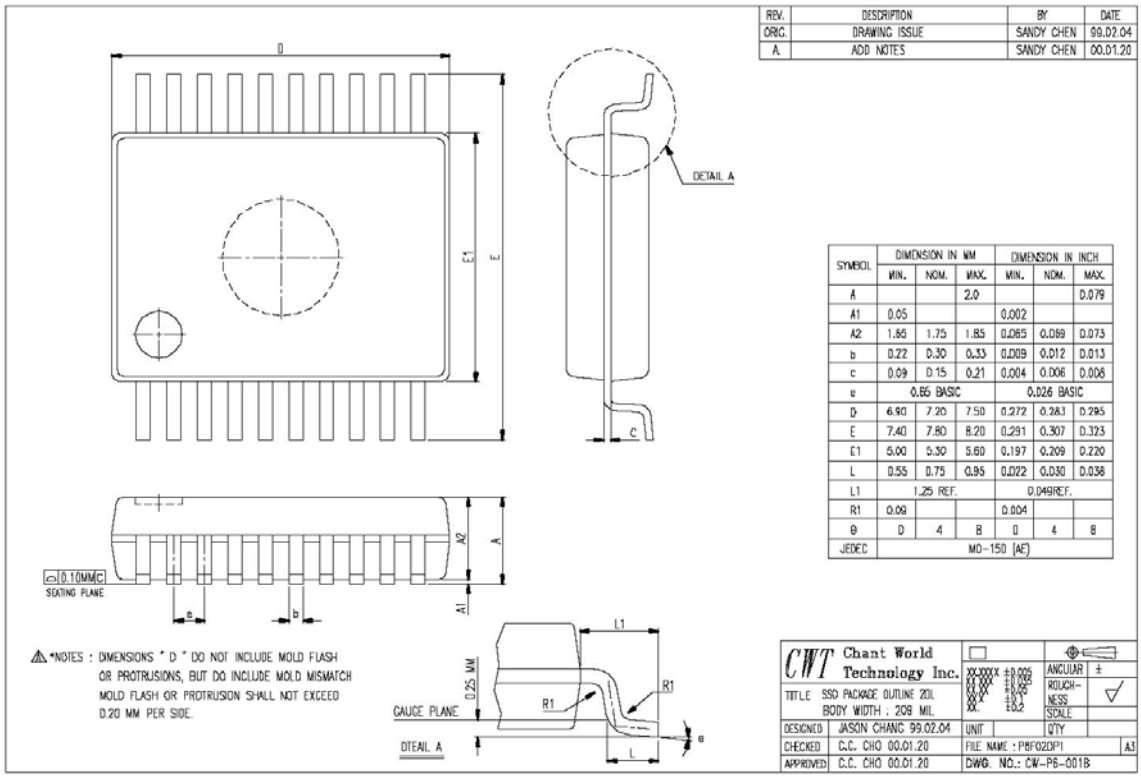
Supply Overvoltage Test

Table 6.5 Latch-Up Data Table

Mode		Voltage (V)/Current (mA)	S/S	Results
Voltage	+	11.0	5	Pass
	-	11.0	5	Pass
Current	+	200	5	Pass
	-	200	5	Pass
Vdd - Vxx		9.0	5	Pass

7.0. Mechanical Information

Figure 7.1 Mechanical Information Diagram



8.0. Abbreviation

This chapter lists and defines terms and abbreviations used throughout this specification.

EEPROM Electrically Erasable Programmable Read-Only Memory

DES Data Encryption Standard

SDK software development kit

SIE Serial Interface Engine

【MEMO】

About Alcor Micro, Corp

Alcor Micro, Corp. designs, develops and markets highly integrated and advanced peripheral semiconductor, and software driver solutions for the personal computer and consumer electronics markets worldwide. We specialize in USB solutions and focus on emerging technology such as USB and IEEE 1394. The company offers a range of semiconductors including controllers for USB hub, integrated keyboard/USB hub and USB Flash memory card reader…etc. Alcor Micro, Corp. is based in Taipei, Taiwan, with sales offices in Taipei, Japan, Korea and California.

Alcor Micro is distinguished by its ability to provide innovative solutions for spec-driven products. Innovations like single chip solutions for traditional multiple chip products and on-board voltage regulators enable the company to provide cost-efficiency solutions for the computer peripheral device OEM customers worldwide.